

<b>DEPARTMENT OF DEFENSE</b> <b>CONTRACT SECURITY CLASSIFICATION SPECIFICATION</b> <i>(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)</i>				<b>1. CLEARANCE AND SAFEGUARDING</b> a. FACILITY CLEARANCE REQUIRED <div style="text-align: center; border: 1px solid black; padding: 2px;"><b>TOP SECRET</b></div> b. LEVEL OF SAFEGUARDING REQUIRED <div style="text-align: center; border: 1px solid black; padding: 2px;"><b>TOP SECRET</b></div>	
<b>2. THIS SPECIFICATION IS FOR:</b> <i>(X and complete as applicable)</i>				<b>3. THIS SPECIFICATION IS:</b> <i>(X and complete as applicable)</i>	
a. PRIME CONTRACT NUMBER  		a. ORIGINAL <i>(Complete date in all cases)</i>		DATE (YYYYMMDD)	
b. SUBCONTRACT NUMBER  		b. REVISED <i>(Supersedes all previous specs)</i>		REVISION NO. 	
X c. SOLICITATION OR OTHER NUMBER <div style="text-align: center;">FA8818-04-R-0012</div>		DUE DATE (YYYYMMDD) 		c. FINAL <i>(Complete Item 5 in all cases)</i>	
<b>4. IS THIS A FOLLOW-ON CONTRACT?</b>		<div style="display: flex; justify-content: space-between;"> <div> <input type="checkbox"/> YES </div> <div> <input checked="" type="checkbox"/> NO. If Yes, complete the following:  Classified material received or generated under _____ <i>(Preceding Contract Number)</i> is transferred to this follow-on contract. </div> </div>			
<b>5. IS THIS A FINAL DD FORM 254?</b>		<div style="display: flex; justify-content: space-between;"> <div> <input type="checkbox"/> YES </div> <div> <input checked="" type="checkbox"/> NO. If Yes, complete the following:  In response to the contractor's request dated _____, retention of the classified material is authorized for the period of _____. </div> </div>			
<b>6. CONTRACTOR</b> <i>(Include Commercial and Government Entity (CAGE) Code)</i>					
a. NAME, ADDRESS, AND ZIP CODE TBD		b. CAGE CODE TBD		c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i> TBD	
<b>7. SUBCONTRACTOR</b>					
a. NAME, ADDRESS, AND ZIP CODE N/A		b. CAGE CODE N/A		c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i> N/A	
<b>8. ACTUAL PERFORMANCE</b>					
a. LOCATION TBD		b. CAGE CODE TBD		c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i> TBD	
<b>9. GENERAL IDENTIFICATION OF THIS PROCUREMENT</b>  Space Test Program (STP) /Standard Interface Vehicle (SIV)  Maj Randolph E. Ripley, Program Manager					
<b>10. CONTRACTOR WILL REQUIRE ACCESS TO:</b>			<b>11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:</b>		
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	YES	NO	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	YES	NO
b. RESTRICTED DATA	X		b. RECEIVE CLASSIFIED DOCUMENTS ONLY		X
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		X	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	X	
d. FORMERLY RESTRICTED DATA	X		d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	X	
e. INTELLIGENCE INFORMATION			e. PERFORM SERVICES ONLY		X
(1) Sensitive Compartmented Information (SCI)	X		f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		X
(2) Non-SCI		X	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	X	
f. SPECIAL ACCESS INFORMATION	X		h. REQUIRE A COMSEC ACCOUNT	X	
g. NATO INFORMATION		X	i. HAVE TEMPEST REQUIREMENTS	X	
h. FOREIGN GOVERNMENT INFORMATION		X	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	X	
i. LIMITED DISSEMINATION INFORMATION		X	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	X	
j. FOR OFFICIAL USE ONLY INFORMATION	X		l. OTHER <i>(Specify)</i>	X	
k. OTHER <i>(Specify)</i>	X		Receive and generate sensitive-but-unclassified information		
DoD Space System Protect Guide Information					

12. **PUBLIC RELEASE.** Any information (*classified or unclassified*) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release ☐ Direct ☒ Through (*Specify*)  
See Annex 1 Para 3, section 12.

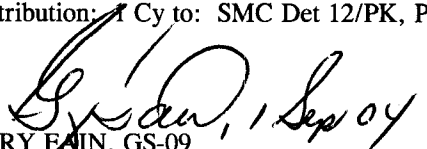
to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)\* for review.  
\*In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. **SECURITY GUIDANCE.** The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (*Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.*)

References to the DoD Industrial Security Manual within the form and the contract are superseded by DoD 5220.22-M, National industrial Security Program Operating Manual (NISPOM). Other security and information protection guidance for application to this contract are attached as follows:

Annex 1, Additional DD 254 guidance  
Annex 2, Special Access Information  
Annex 3, Sensitive Compartmented Information  
Annex 4, Communication Security Measures  
Annex 5, Emissions Security Measures (AFI will be furnished under separate cover)  
Annex 6, Other Security and Protection Measures

Distribution: 1 Cy to: SMC Det 12/PK, PKT, ST, STS, MSS

  
GARY FAIN, GS-09  
SMC Det 12 Security Manager

14. **ADDITIONAL SECURITY REQUIREMENTS.** Requirements, in addition to ISM requirements, are established for this contract. ☒ Yes ☐ No  
(*If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.*)

See Annex 1

15. **INSPECTIONS.** Elements of this contract are outside the inspection responsibility of the cognizant security office. ☒ Yes ☐ No  
(*If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.*)

See Annex 1

16. **CERTIFICATION AND SIGNATURE.** Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL  
ODETTE G. DENMAN, GS-13, DAF

b. TITLE  
Contracting Officer

c. TELEPHONE (*Include Area Code*)  
(505) 846-9147

d. ADDRESS (*Include Zip Code*)  
SMC Det 12/PKT  
3548 Aberdeen Ave SE  
Kirtland AFB, NM 87117

17. **REQUIRED DISTRIBUTION**

- |                                     |   |
|-------------------------------------|---|
| <input checked="" type="checkbox"/> | a. CONTRACTOR   |
| <input type="checkbox"/>            | b. SUBCONTRACTOR  |
| <input checked="" type="checkbox"/> | c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR          |
| <input type="checkbox"/>            | d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION |
| <input checked="" type="checkbox"/> | e. ADMINISTRATIVE CONTRACTING OFFICER                             |
| <input checked="" type="checkbox"/> | f. OTHERS AS NECESSARY  |

e. SIGNATURE

**ANNEX 1**  
**CONTRACT SOLICITATION NO. FA8818-04-R-0012**  
**DD FM 254 GUIDANCE**

Remarks pertaining to Sections 10, 11, 12, 13, 14, and 15 are as follows:

**1. SECTION 10:**

**1.1** Contractor personnel must possess a final U.S. Government clearance at the appropriate level and be briefed (as required) for access to classified information. A list of Contractor personnel with such accesses will be provided to the SMC Det 12 Security Office upon request. Visit requests must identify access granted and date last briefed. The contractor shall apply all applicable markings to the material to include warning notices. All data and materials will be handled, disclosed, transmitted, reproduced and stored in accordance with the NISPOM and organizational guidance.

**Item 10a:** COMSEC Information - see Annex 4 for further instructions

**Item 10e.** Sensitive Compartmented Information- See Annex 3 for further instructions

**Item 10f.** Special Access Information - see Annex 2 for further instructions

**Item 10h.** Foreign Government Information. **RELEASE OF CLASSIFIED AND UNCLASSIFIED INFORMATION TO FOREIGN GOVERNMENT AND THEIR REPRESENTATIVES:** Any military activity or defense contractor receiving a request from a foreign government, or a representative thereof, for classified and/or unclassified information about this program shall forward the request to through SMC Det 12/ST to SMC Det 12 MSS (Foreign Disclosure Office) for approval. This does not apply to exchange or information on approved foreign military sales programs.

**Item 10j:** DoD 5400.7/AF Sup 1, Chap 4 governs For Official Use Only information. Additionally, guidance for the transmittal of sensitive but unclassified or controlled unclassified across the Internet may be found in AFI 33-129.

**2. SECTION 11:**

**2.1 Item 11c:**

**2.1.1** All personnel assigned to this effort and handles classified information must be a U.S. citizen and have a minimum of a final SECRET security clearance. A limited number of personnel must have and able to hold a current (no older than 5 years) TOP SECRET clearance.

**2.1.2** The contractor will require access to TOP SECRET source data in support of this work effort. Any extracts or use of such data will require the contractor to apply derivative classifications and markings consistent with the source from which the extracts were made.

**2.1.3** See under Contract Clauses of the contract, Notification of Government Security Activity Clause, Part II. Work, to include classified automatic data processing, will be accomplished at prime contractor facilities, Kirtland AFB, and other locations designated by the government. When processing classified information on government furnished automated information systems (AIS) the contractor shall comply with all applicable DOD, Air Force, Major Commands and local Security and Protection Guidelines. It is the contractor's responsibility to understand these publications (e.g., directives, instructions, manuals, plans) and obtain either a hard copy or soft copy from the office providing support to, i.e., the Contracting Officer, Security Office, and/or Information Assurance Office.

**2.2** **Item 11j:** Operations Security (OPSEC) is an unclassified program design to deny our adversaries access to critical information. OPSEC implementation is an inherent responsibility for all personnel that handles For Official Use Only information and other categories of sensitive information. The government has the responsibility to integrate OPSEC into plans, directives and to develop policy, provide guidance and training. OPSEC education shall be provided to all personnel as part of in-processing and on an annual basis. General environmental awareness and proper safeguarding is the vital link to protect our critical assets. Contractors shall be required to comply with the Det 12 OPSEC Instruction and assigned program Critical Indicator Profile in performance of day-to-day duties.

**2.3** **Item 11l:** Sensitive-but-Unclassified (SBU) automatic data processing will occur at the prime contractor facilities, Kirtland AFB and other locations designated by the government. The contractor will also be granted access to networks at these locations or interface between these sites via the Internet. When processing SBU information on either government-furnished or contractor systems, ADPE prior approval must be granted by the SMC Det 12 Information Assurance Office. Information of an SBU nature will not be placed on the Internet without approved and tested access and security controls. This includes information that falls under the definition of Personal or Privacy Act, For Official Use Only, Scientific, Technical or Research and Development.

### **3. SECTION 12:**

There will be no voluntary public release of information. Requests for public release of information concerning this contract shall be submitted through SMC Det 12/ST to SMC Det 12/CCX 45 days in advance of scheduled release date. Answers to queries may be made only with the express approval of the SMC Det 12/CCX, 3548 Aberdeen Ave SE, Kirtland AFB NM 86117-5606. No other dissemination of information is authorized. This prohibition extends to all publications of an informational nature both internal and external, and to all conversations except those required for conduct of official business.

**4. SECTION 13:**

**4.1** Classified information may be transmitted through the Internet if encrypted utilizing National Security Agency approved encryption methods. Only releasable public information may be directly accessed from the Internet without access and/or security controls. All information maintained on a computer system connected to the Internet and not protected by access controls must be public access information.

**4.2** Refer to Annex 6, Other Security and Protection Measures with regard to Security Classification Guidance and Program Protection Information.

**5. SECTION 14:** Additional security requirements, in addition to the NISPOM and associated annex(es), are established. Refer to the appropriate annex to the DD Fm 254 for these requirements and guidelines.

**6. SECTION 15:** The Defense Security Service retains inspection responsibilities for all collateral information in the contractor's facility. SMC Det 12 Information Protection Office, 3548 Aberdeen Ave SE has inspection responsibility for all unclassified and SBU materials within the contractor's facility.

**ANNEX 2**  
**CONTRACT SOLICITATION NO. FA8818-04-R-0012**  
**SPECIAL ACCESS INFORMATION**

**1. Special Access Information:**

a. The contractor shall establish a point of contact for Special Access Required (SAR) security matters. This individual will have responsibility for all SAR security matters within the contractor's facility, in accordance with the appropriate SAR Security Guide.

b. The contractor shall establish and maintain an access list of those employees approved by the contract monitor for SAR portions of the contract. A copy of this list will be furnished to SMC Det 12 Security Office.

c. The contractor will advise SMC Det 12 Security Office and immediately upon reassignment of SAR accessed personnel to other duties not associated with this contract.

**ANNEX 3**  
**CONTRACT SOLICITATION NO. FA8818-04-R-0012**

**SENSITIVE COMPARTMENTED INFORMATION**

**1. GENERAL**

**a. Physical Security**

This contract requires access to Sensitive Compartmented Information (SCI). The assistant Chief of Staff for Intelligence, USAF, has exclusive security responsibility for all SCI classified material released to or developed under this contract. This SCI information must be maintained in a Sensitive Compartmented Information Facility (SCIF). DCID 6/4, 6/9, DoD 5105.21-M-1 and AFM 14-304 serves as the necessary guidance for physical, personnel, and information security measures and are part of the security specification for this contract. Contractor compliance with these directives is mandatory unless specifically waived. Inquiries pertaining to classification guidance for SCI will be directed to SMC/INS through the Contract Monitor. The contractor is required to comply with the physical security standards as defined in DCID 6/9, DOD 5105.21-M-1 and AFM 14-304. SCI material released to the contractor under this contract shall be stored and worked on only within the proposed facility and upon receipt of an approved physical security accreditation by SSO DIA/DAC. AFSPC sponsored SCIF shall not be co-utilized with other government agencies unless covered by an approved Co-Utilization Agreement (CUA). The User Agency SSO is SMC/INS, Los Angeles AFB, CA. Work performed under this contract shall not be accomplished in a SCIF accredited by another Government Organization unless there is an approved CUA between that organization and SMC/INS. Applicable Program Security Classification guidance will be identified in block 13 of this DD Form 254.

**b. Personnel Security**

The contractor shall nominate a CSSO and Alternate to SMC/INS. No contractor will be granted access to SCI information/material under this contract unless they are filling a SMC/IN SCI billet assigned under this contract. The names of contractor personnel requiring accessing to SCI will be submitted to SMC/INS through the Contract Monitor. Upon receipt of a completed background investigation the CSSO will submit a request for SCI eligibility to SMC/INS in accordance with AFM 14-304. Contract employees sponsored by other than Agencies/Organization shall be certified to SMC/INS through the Servicing SSO for access to a SMC Programs. The contractor shall establish and maintain a current billet roster indicating accesses of SCI personnel on this contract. A copy of this list shall be provided to SMC/INS through the Contract Monitor annually, or as changes occur. The contractor shall also advise SMC/INS through the Contract Monitor immediately upon the reassignment of personnel to duties not associated with this contract, to include termination.

**c. Document Control**

SCI furnished in support of this contract remains the property of the SMC Program Office releasing it. The contractor shall maintain an active accountability of all SCI material received, produced, maintained, and disposed of that is in their custody. Upon completion or cancellation of this contract, SCI data will be returned to the custody of the government (Program Office) unless a follow-on contract specifies that material will be transferred to that contract. Inventories of SCI material will be conducted in accordance with DOD 5105.21-M-1 and AFM 14-304. Any supplemental instructions will be furnished and/or made available to the contractor through the Contract Monitor by the User Agency Special Security Office (SMC/INS)

**d. Release of Information**

SCI will be released to contractors only when originator approval has been obtained. The contractor may release such material to any contractor employee assigned to a billet and indoctrinated for Program SCI access under this contract and only when a need-to-know exists. The contractor may release such material to any Special Security Office personnel assigned to HQ SMC, HQ Air Force Space Command (AFSPC), HQ USAF, or DIA upon demand. The contractor shall not release this material to other contractor, subcontractor, or Federal Government agency employees unless the Program Office, Contract Monitor, or SMC/INS has granted prior written approval. An access certification to an SMC contractor occupied SCIF does not constitute approval to release SMC contractual material to other contractor, subcontractor, or federal government employees: SMC/INS or Contract Monitor approval is required. SCI will not be released to non-U.S. citizens. SMC/INS approval of an SMC contractor visit certification or permanent certification to another facility will constitute approval to discuss contractual information/material at the facility to be visited.

**e. Reproduction of SCI Information**

The contractor may reproduce any SCI related to this contract at the discretion of the Contract Special Security Officer (CSSO), as long as the copies are controlled in the same way as the originals and they remain in the SCIF. No copies of SCI documents will be transferred to other contractors.

**f. Sub-Contracting**

A CSSO shall coordinate with the Contract Monitor and obtain the concurrence of SMC/INS prior to subcontracting any portion of SCI efforts involved in this contract.

**g. Public Release**

The contractor shall not make references to SCI even by unclassified acronyms, in advertising, promotional efforts, or recruitment for employees.



2. **BLOCK 10k: Other: Automated Information Systems**

Comply with DOD 5105.21-M1 Chapters 7 and 8, DIAM 50-4, AFM 14-304 Chapters 7 & 8. The Contractor CSSO shall submit a Systems Security Concept of Operations and an AIS Security Operations Procedure/Standard Practice Procedure.

3. **BLOCK 11i TEMPEST Requirements**

TEMPEST security measures must be considered if electronic processing of SCI is involved in accordance with DOD 5105.21-M1 Chapter 7 and Appendix J; AFM 14-304, Chapter 7

4. **BLOCK 11k Defense Courier Service**

This contract requires the use of the Defense Courier Service (DCS). The CSSO will prepare and submit DCS Form 10 in original triplicate to SSO SMC/INS for validation prior to their submittal to the appropriate DCS station (reference to Block 11k).

5. **BLOCK 14 Additional Security Requirements**

The following Directives, Manuals, Instructions, Handbook, or Pamphlet are incorporated into this contract as they pertain to the access, handling, control, dissemination, processing of Sensitive Compartmented Information:

DCID 6/4  
DCID 6/9  
DOD 5105.21-M1  
DIAM 50-4  
AFM 14-304

6. **BLOCK 15 Inspections**

Defense Security Service is relived of inspection responsibilities pertaining to Sensitive Compartmented Information associated with this contract. The following activity is designated as inspection authority and the User Agency SSO for SCI requirements in accordance with DOD 5105.21-M-1, and AFM 14-304.

SMC/INS (SMC SSO)  
2420 Vela Way, Suite 1467  
Los Angeles AFB  
El Segundo, CA 90245-4659

The User Agency Special Security Officer (SSO) is: SMC/INS (310) 363-0175  
The Alternate Special Security Officer (ASSO) is: SMC/INS (310) 363-1585

**ANNEX 4**  
**CONTRACT SOLICITATION NO. FA8818-04-R-0012**

**COMMUNICATIONS SECURITY (COMSEC) MEASURES**

**1.0    GENERAL.** The contractor shall, in addition to the requirements set forth in the DoD National Industrial Security Program Operating Manual (NISPOM) (DoD 5220.22-R), and the COMSEC Annex (DoD 5220.22-S) comply with the written instructions of the installation Commander regarding communications security matters.

**2.0    PURPOSE.** Provides for additional security measures required by the Government to be taken to deny unauthorized persons information derived from telecommunications of the U.S. Government relating to national security and to ensure the authenticity of such communications. COMSEC protection results from the application of security measures to electrical systems which generate, handle, process, or use national security information.

**3.0    REFERENCE.** Item 11h of the DD Fm 254

**4.0    COMSEC AND/OR CRYPTOGRAPHIC ACCESS**

**4.1**    COMSEC material/information may not be released to DoD contractors without Air Force Cryptological Support Center (AFCSC) approval. Contractor must forward request for COMSEC material/information to the COMSEC Officer through the program office. The contractor is governed by NSAM 90-1, Oct 2001 for the control and protection of COMSEC material/information. Access to COMSEC material/information is restricted to U.S. citizens holding final U.S. government clearances and is not releasable to personnel holding only a reciprocal clearance.

**4.2**    The Air Force program/project manager shall designate the number of personnel requiring cryptographic access. The number will be limited to the minimum necessary and will be on a strict need-to-know basis.

**4.3**    The COMSEC/CRYPTO briefing applies only to the use and control of crypto equipment and specialized COMSEC publications. NACSIM/NACSEM documents are not considered COMSEC controlled material. Additionally, cryptographic information/equipment will not be retained in a contractor facility.

**5.0    INTERNET POLICY AND ENCRYPTION**

**5.1**    Classified information may be transmitted through the Internet if encrypted utilizing National Security Agency approved encryption methods. Only releasable public information may be directly accessed from the Internet without access and/or security controls. All information maintained on a computer system connected to the Internet and not protected by access controls, must be public access information.

SOLICITATION, 1 September 2004

**ANNEX 5**  
**CONTRACT SOLICITATION NO. FA8818-04-R-0012**

**EMISSIONS SECURITY (EMSEC) MEASURES**

AFI submitted under separate cover.

**ANNEX 6**  
**CONTRACT SOLICITATION NO. FA8818-04-R-0012**  
**OTHER SECURITY AND PROTECTION MEASURES**

**1.0 SECURITY CLASSIFICATION GUIDES**

Security Classification Guides (SCG) to include any changes or revisions will be made available to the contractor in performance of contractual tasks as required.

**2.0 PROTECT GUIDES**

The National Security Policy and DoD Space Policy and supplements require RDT&E entities develop protect guides for major systems and support capabilities. This is an effort to reduce the number of SCGs and focus information classification at the system level. Applicable SCG content however will be considered when developing protect guides for SMC Det 12. Protect guides are also developed for modernization and development, test and operations purposes. Contractor agencies will be required to participate (i.e., provide existing documents and attend meetings) in applicable protect guides development. Protect guides to include any changes or revisions will be made available to the contractor in the performance of contractual tasks as required.

**3.0 PROGRAM PROTECTION PLAN**

A Program Protection Plan (PPP) is required in accordance with the Acquisition Security Program. The Air Force will integrate security needs and requirements into a PPP beginning in Phase 0 of an acquisition program and maintain this plan throughout the system's life. Contractor agencies will be required to participate (i.e., provide existing documents and attend meetings) in applicable PPP development. The PPP to include any changes or revisions will be made available to the contractor in the performance of contractual tasks as required.

**4.0 ORIGINAL CLASSIFICATION AUTHORITY (OCA) AND  
DECLASSIFICATION AND DOWNGRADING AUTHORITY (DDA)**

**4.1 Delegation and Authorization.** The Secretary of the Air Force is responsible to make appointments and delegations, in accordance with Executive Order 12958, of those Air Force positions authorized to originally classify and declassify or downgrade classified information and their level of authority. For example, only an OCA can classify information at the level authorized, and only a DDA can authorize declassification or downgrading of that information. The contractor's classification of information is derivative to the original guidance, and actions to declassify or downgrade this information should be in accordance with DDA

guidance. This guidance is generally provided in the form of an SCG but may also be provided by other written medium.

**4.2 Classification Challenges.** Requests to challenge information classification, or to have information declassified or downgraded outside of its specified time, should be submitted through the SMC Det 12 Security Office for OCA and DDA action. Pending an OCA or DDA reply the classified information will be handled at its current level of classification.

## **5. INTERNATIONAL PROGRAMS SECURITY**

The contractor shall ensure full compliance with DOD (e.g., DODD 5230.11), AFI 61-201, and AFI 61-204), supporting major commands supplements and local guidance on International Program security requirements. Applicable guidance will be timely implemented and enforced to effect proper access and protection of affected government functions under this contract. This includes import/export, documentation and technology marking (e.g., warning, distribution, statements, FOIA requirements), discussions and meetings with foreign entities to include those via networks and other related international program security requirements. Any classified or controlled unclassified military information (CUMI), also known as controlled export technical data, and technology to be released must have approved by the Foreign Disclosure Office prior to release. The contractor shall ensure full compliance with the International Traffic in Arms Regulations, and must be able to obtain and maintain the necessary license and agreements (e.g., technical assistance agreement) required in support of this contract.

## **6. NATIONAL SECURITY INFORMATION MARKING**

Executive Order 12958 requires that classified national security information be marked to place recipients on alert regarding its sensitivity. The pamphlet that provides guidance on these marking requirements is available through the contracting office.